Capítulo noveno

Aplicación de COMINT en el marco de la amenaza del crimen organizado en conflictos híbridos

Juan de Dios Gómez Gómez

Resumen

Recientemente, han visto la luz dos documentos de la máxima trascendencia estratégica en lo que se refiere a la seguridad de la UE y de España, la *Brújula Estratégica* (UE) y la *Estrategia de Seguridad Nacional* (España). Ambos identifican la amenaza híbrida como una de las más relevantes a las que la UE y sus Estados miembros deben hacer frente con nuevas estrategias y medidas. En esta línea, una reciente resolución del Parlamento Europeo llama a la Comisión Europea a tomar medidas para identificar y neutralizar este tipo de amenazas. Esta investigación trata de determinar nuevas maneras de explotar las capacidades de inteligencia de comunicaciones (COMINT) desde el escrupuloso respeto a los DDFF de los ciudadanos y con el máximo impacto neutralizador y disuasorio que el Parlamento Europeo busca. La investigación concluye con una serie de propuestas de medidas concretas para alcanzar dicho objetivo y de nuevas líneas de investigación.

Palabras clave

Inteligencia, Conflictos híbridos, Crimen organizado, Zona gris, Derechos Fundamentales.

Application of COMINT in the context of the organised crime threat in hybrid conflcts

Abstract

Two documents of the utmost strategic importance in terms of the security of the EU and Spain have recently been published: the Strategic Compass (EU) and the National Security Strategy (Spain). Both identify the hybrid threat as one of the most relevant threats that the EU and its Member States must address with new strategies and measures. In this sense, a recent resolution of the European Parliament calls on the European Commission to take measures to identify and neutralize this type of threat. This research aims to identify new ways to exploit communications intelligence (COMINT) capabilities while scrupulously respecting the DDFF of citizens and with the maximum neutralizing and deterrent impact sought by the European Parliament. The study concludes with a series of proposals for concrete measures to achieve this objective and for new lines of research.

Key words

Intelligence, Hybrid conflicts, Organized Crime, Gray zone, Fundamental Rights.

1. Introducción

La amenaza del crimen organizado en el ámbito de conflictos híbridos sostenidos en Estados vulnerables, desestabilizados, caídos, en situación poscrisis o en proceso de recuperación, puede contribuir a la ausencia o pérdida de confianza en los poderes públicos de dichos países. En ocasiones, incluso entrelazando sus actividades y fines con el terrorismo o la subversión. También en Estados democráticos consolidados, el crimen organizado puede erigirse en una herramienta al servicio de intereses desestabilizadores o, por qué no, de agresión manifiesta, operando en una zona gris del conflicto. Las organizaciones criminales tienen a su alcance muy relevantes capacidades para proveer de seguridad sus sistemas de comunicaciones y preservar sus actividades e informaciones más sensibles fuera del alcance de las agencias implicadas en combatirlas y de los poderes públicos.

El Parlamento Europeo está preocupado por la falta de normas, medidas y medios de la UE y de sus Estados miembros para prevenir, detectar, atribuir, contrarrestar y sancionar actos de injerencia extranjera. Estos actos incluyen injerencias extranjeras en procesos electorales, financiación encubierta de actividades políticas por parte de actores donantes extranjeros y ciberataques, entre otros (INGE Consolidated Draft Report, 2022: 7-21).

Actualmente, la UE no cuenta con un marco legal que tipifique como ilícitas estas acciones de injerencia extranjera y les asigne un régimen sancionador que evite que los actores que hoy en día las llevan a cabo queden impunes. Consciente de ello, el Parlamento Europeo trabaja para poner remedio a esta situación y valora el establecimiento de sanciones de tipo comercial que puedan aplicarse de manera transparente y con todas las garantías del derecho internacional, con plena conciencia de que este tipo de acciones de injerencia son ataques de naturaleza híbrida que quedan por debajo del umbral del apartado 7 del artículo 42 del Tratado de la Unión Europea y del artículo 5 del Tratado del Atlántico Norte (INGE Consolidated Draft Report, 2022).

Este trabajo pretende explorar nuevas líneas de mejora de capacidades COMINT aplicables a la lucha contra el crimen organizado en el marco de conflictos híbridos. La novedad de la amenaza que estos escenarios implican para la defensa de los Estados exige una adaptación por parte de estos en tanto a la implementación de nuevas y más adaptadas y eficientes capacidades. Por ello se plantea este objetivo con la voluntad de

contribuir a mejorar las capacidades de inteligencia de comunicaciones que puedan ser empleadas para contrarrestar y neutralizar estas amenazas.

2. Estado actual de la cuestión

La Oficina de las Naciones Unidas contra la droga y el delito, en su Estrategia 2021-2025, constata que la delincuencia organizada y la corrupción siguen socavando la estabilidad, la paz y la seguridad, lo que ha dado lugar a un aumento de la violencia, la desestabilidad y el debilitamiento de los Estados. Del mismo modo, afirma, la financiación y las operaciones de los grupos terroristas a menudo dependen de actividades delictivas organizadas, como el tráfico de armas.

Gabriel Martínez Velara, en su trabajo «Actores no estatales en la zona gris», considera que las organizaciones de carácter violento y crimen organizado transnacional (2018) instan a abordar los cambios organizativos y legales que permitan actuar de manera coordinada e integrada frente a esta amenaza híbrida, y anima, en especial, a restringir los tráficos ilegales y la actuación de las organizaciones del crimen organizado transnacional para evitar que faciliten la financiación de los actores no estatales violentos que pueden actuar en la zona gris de los conflictos.

Una publicación del *think tank* European Council on Foreing Relations elaborada por Mark Galeotti, *Crimintern: How the Kremlin uses Russia's criminal networks in Europe* (2017), describe como grupos criminales organizados rusos han sido empleados por el Kremlin como instrumentos de actividades de inteligencia e influencia política.

La situación de la obtención de inteligencia criminal sobre el crimen organizado queda meridianamente patente en recientes publicaciones llevadas a cabo por EUROPOL. En diciembre de 2021, la referida agencia europea, hacía públicas las cinco operaciones contra el crimen organizado más destacadas llevadas a cabo en el citado año[1]. Dos de ellas, la operación Troyan Shield/ Greenlight y la operación Sky ECC, tuvieron como objetivo principal la toma del control de las comunicaciones cifradas de las organizaciones criminales. Otra, la operación Jumita, llevó a cabo

[1] Disponible en: https://www.europol.europa.eu/media-press/newsroom/news/europol%E2%80%99s-highlights-of-2021-year-in-review

la desarticulación de una gran organización criminal de tráfico de drogas en el Campo de Gibraltar como consecuencia de la inteligencia obtenida de medidas de investigación tecnológica basadas en las comunicaciones electrónicas empleadas por los criminales; y, una cuarta, tuvo lugar en el ciberespacio desactivando el *botnet* EMOTET[2].

No en vano, EUROPOL describe en su *Serious and Organised Crime Threat Assessment* del pasado año 2021 cómo las organizaciones criminales han hecho uso de comunicaciones encriptadas y de soluciones especializadas, diseñadas e implementadas de manera dedicada para proteger la seguridad de sus comunicaciones electrónicas ante el ejercicio del derecho de injerencia de los Estados mediante sus actividades de lucha contra la criminalidad.

3. Capacidades COMINT en la lucha contra el crimen organizado

3.1. El uso de las comunicaciones electrónicas por parte del crimen organizado

Las comunicaciones electrónicas han supuesto una extraordinaria oportunidad para el crimen organizado a nivel global, ofreciéndole enlace global para coordinar sus actividades ilícitas transnacionales y, todo ello, alcanzando niveles de seguridad y confidencialidad insospechados hace décadas gracias al cifrado y a la *anonimización* de las conexiones a la red. En este sentido, los Estados democráticos han tenido y tienen que hacer grandes esfuerzos para evitar que esta oportunidad para el crimen organizado no devenga en una brecha de seguridad nacional o transnacional, dotándose de las herramientas necesarias para poder materializar su derecho legítimo a injerir en el derecho al secreto de las comunicaciones de los ciudadanos cuando el bien común de la seguridad nacional o la seguridad pública lo justifica, y todo ello de manera eficaz. Cada vez más, las capacidades COMINT avanzadas son más necesarias para la inteligencia procesal penal y para la seguridad nacional.

La última tendencia en el mundo del crimen organizado, para dotarse de comunicaciones secretas, es el uso de soluciones

[2] Disponible en: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

ad hoc, especialmente diseñadas para el uso criminal. Según EUROPOL: «Las redes delictivas tienen una gran demanda de plataformas de comunicación cifradas para facilitar sus actividades delictivas» (EUROPOL, 2021). Ejemplos de ello son los sistemas ENCROCHAT o Sky ECC, que fueron empleados durante años por los criminales en todo el mundo sin que nada pudieran hacer las agencias dedicadas a combatir el crimen para interceptar en claro el contenido de sus comunicaciones.

Prueba de la extraordinaria relevancia adquirida por las capacidades COMINT en la lucha contra el crimen organizado son algunas de las operaciones transnacionales más relevantes llevadas a cabo en el pasado año 2021 en Europa y destacadas por la agencia europea EUROPOL en su página web. En dicha web se destacan tres operaciones: las mencionadas, en las que las COMINT fueron trascendentales. La Operación JUMITA, fundamentada en COMINT y llevada a cabo por la Guardia Civil en España, concluyó con el desmantelamiento de una red criminal dedicada al tráfico de cocaína con origen en América del Sur y destino al puerto de Algeciras, la detención de 29 personas, la aprensión de 1.6 toneladas de cocaína y la confiscación de 16.5 millones de euros. El desbloqueo de la encriptación de la solución Sky ECC llevado a cabo por Bélgica, Francia y Países Bajos es otra de las grandes operaciones destacada por EUROPOL en 2021.

Y, por último, EUROPOL destaca la operación TROJAN SHIELD/ GREENLIGHT, una de las mayores y más sofisticadas operaciones policiales realizada hasta la fecha en la lucha contra las actividades delictivas cifradas. Esta operación fue llevada a cabo por la Oficina Federal de Investigación de Estados Unidos (FBI), la Policía Nacional de los Países Bajos (Politie) y la Autoridad Policial de Suecia (Polisen), en cooperación con la Administración para el control de drogas de Estados Unidos (DEA) y otros 16 países, entre ellos España y, en concreto, la Guardia Civil. Desde 2019, la Oficina Federal de Investigación de Estados Unidos, en estrecha coordinación con la Policía Federal Australiana, desarrolló estratégicamente y operó de forma encubierta una empresa de dispositivos cifrados, llamada ANOM, que llegó a dar servicio a más de 12.000 dispositivos cifrados usados por más de 300 sindicatos delictivos que operaban en más de 100 países, entre ellos la delincuencia organizada italiana, las bandas de motoristas ilegales y las organizaciones internacionales de tráfico de drogas.

3.2. Técnicas COMINT en el ámbito de la interceptación legal de comunicaciones: COMINT dirigido

3.2.1. COMINT vía proveedores de servicios de comunicaciones

La principal característica de este procedimiento COMINT es que, para la obtención de la información o los datos de una comunicación objetivo, se requiere la cooperación del proveedor de servicios de la información o del operador de red de comunicaciones que haya gestionado a nivel técnico la transmisión del mensaje. En el caso de la telefonía móvil, que es el más habitual en el ámbito de la lucha contra el crimen organizado, nos referiremos a las compañías operadoras de las redes celulares, fijas o satelitales de telefonía. En la Unión Europea este es un ámbito profusamente regulado, tanto a nivel de normativa referente a la protección de los DDFF de los ciudadanos, relativos al secreto de las comunicaciones[3] y a la protección de datos personales[4], como a nivel técnico con normativa que establece estándares técnicos para el intercambio de información entre las operadoras y las autoridades nacionales responsables de ejecutar las medidas de investigación basadas en la interceptación de las comunicaciones[5].

Otra característica de este tipo de interceptación es su carácter dirigido, es decir, no masivo. Esta medida de investigación se justifica legalmente y se ejecuta de manera dirigida a un individuo en concreto y siempre bajo la premisa de la existencia de indicios racionales de criminalidad que justifiquen la intromisión en el derecho al secreto de las comunicaciones. Estos requisitos son fácilmente reconocibles en la legislación procesal penal española. Pueden apreciarse fácilmente de la lectura del Artículo 588 bis b de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de

[3] Véase la Sentencia Del Tribunal Europeo de Derechos Humanos sobre el Caso Malone Contra el Reino Unido, 1984, pionera en el reconocimiento de este derecho aplicado a las comunicaciones telefónicas y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de Julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (directiva sobre la privacidad y las comunicaciones electrónicas), 2002.

[4] Véase el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo –de 27 de abril de 2016– relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/ 46/ CE (Reglamento General de Protección de Datos), 2016.

[5] Estándares emitidos por el European Telecommunications Standards Institute (ETSI), en lo relativo a Interceptación Legal (LI) de comunicaciones, véase: https://www.etsi.org/technologies/lawful-interception

Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

En la actualidad la explotación de este tipo de medidas suele llevarse a cabo de manera centralizada por agencia, de forma que cada agencia cuenta con un sistema centralizado donde recibe los datos de todas las interceptaciones en vigor procedentes de las compañías operadoras. En el caso de España el sistema es conocido como SITEL. Este sistema ve la luz desde el punto de vista jurídico en el Real Decreto 424/2005, de 15 de abril, por el que se aprueba la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, y ha sido respaldado por no pocas sentencias del Tribunal Supremo español[6]. Cada agencia española, para ejecutar este tipo de medida COMINT cuenta con un sistema independiente que no tiene conexión directa con ninguno de los del resto de agencias.

3.2.2. COMINT dirigido mediante procedimientos tácticos

En este epígrafe se tratarán aquellos procedimientos COMINT que, también de forma dirigida, se llevan a cabo por parte de las autoridades facultadas legalmente para ello, esta vez sin cooperación ni participación de las operadoras de redes de comunicaciones o proveedores de servicios de información de ningún tipo. Evidentemente, al prescindirse de la cooperación de terceros en la ejecución de esta medida, se gana en discreción y confidencialidad, pero, por otro lado, este tipo de procedimientos exigen un mayor esfuerzo táctico y operativo para su ejecución.

Desde el punto de vista jurídico, podría decirse que el alcance de esta medida es análogo al de la tratada en el epígrafe interior, pues la manera en la que afecta a los DDFF de los ciudadanos es idéntica, existiendo solo diferencias respecto al procedimiento técnico de ejecución.

Estos procedimientos suelen precisar medios técnicos y despliegues tácticos que permiten acceder a los canales de la comunicación empleados por los terminales de comunicaciones usados por los individuos objeto de la investigación de forma directa por parte de la autoridad que ejecute la medida.

El valor añadido de este tipo de modalidad COMINT es que puede ejecutarse de manera autónoma en cualquier lugar sin necesidad

[6] Véase STS 279/2017, 19 de abril de 2017.

de acuerdo de cooperación ni infraestructura de conexión con ningún tercero. Las únicas prevenciones para tener en cuenta se refieren a la tecnología empleada por los medios técnicos propios de las agencias ejecutantes de la medida que deban ser desplegados[7]. Además, estos medios técnicos pueden desplegarse desde una gran variedad de plataformas, bien sean aéreas[8], terrestres o navales. Por tanto, es un procedimiento flexible, ágil y versátil, que puede ser aprovechado en multitud de entornos y escenarios.

3.2.3. Retención de datos asociados a las comunicaciones como procedimiento COMINT

Además del contenido material de una comunicación que constituye el mensaje que el emisor quiere hacer llegar al receptor, existe toda una serie de datos asociados a una comunicación que pueden ser de extraordinario valor informativo. Incluso no conociendo el contenido de un mensaje, si se dispone de datos asociados a la comunicación como la identidad de emisor y receptor, la ubicación geográfica de los transmisores y receptores en el momento de la comunicación, la fecha y hora de la comunicación, el tipo de comunicación, la duración de la comunicación, etc., pueden alcanzarse muy relevantes conclusiones sobre unas hipotéticas necesidades de inteligencia a las que se pretenda dar respuesta. Seguiremos la definición de datos asociados a las comunicaciones electrónicas propuesta por Vallés Causada (2013) [9].

[7] En el caso de telefonía móvil, atenderíamos a las bandas y tecnologías empleadas por las operadoras de redes de comunicaciones celulares en la zona de operación.

[8] Según manifestaciones de miembros del contingente español desplegado en Letonia, como parte del contingente aliado como Presencia Avanzada Reforzada de la OTAN, este tipo de despliegue mediante plataformas aéreas pudo ser empleado por Rusia, véase: https://www.elespanol.com/espana/20220129/soldados-espanoles-frontera-rusia-usan-hackearnos-telefonia/645935817_0.html (Cedeira, 2022).

[9] Vallés Causada (2013) define este tipo de dato de la siguiente forma: «Se entenderá por datos asociados a las comunicaciones electrónicas aquellos datos, distintos del contenido material del mensaje trasmitido, que sean o hayan sido tratados a efectos de la conducción de una comunicación prestada a través de una red de comunicaciones electrónicas por un servicio telemático de la sociedad de la información, incluidos servicios de valor añadido, así como los demás datos afines relativos a la suscripción de cualquiera de estos servicios y los demás producidos por cualquier dispositivo técnico apto para mantener una comunicación electrónica, aun cuando no se vinculen a una comunicación concreta» (Vallés Causada, 2013: 319).

Para conocer más sobre este tipo de medidas COMINT, atenderemos al criterio jurídico del Derecho de la Unión Europea que ha tratado con profusión este asunto en los últimos años.

La Directiva 2002/58/CE Del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a La protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) promulga la posibilidad de que los estados establezcan legislaciones que permitan la conservación de este tipo de datos en su artículo 15.

Con este artículo, el Derecho de la Unión Europea autoriza a los Estados miembros a crear leyes que permitan la conservación de datos asociados a comunicaciones electrónicas. Bien es cierto que con el paso de los años ha sido preciso que el Tribunal de Justicia de la Unión Europea acote y concrete con su interpretación el alcance de esta figura. Así, en la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 21 de diciembre de 2016, dicha autoridad se opone a que las normativas nacionales permitan la conservación masiva e indiscriminada de datos asociados a las comunicaciones, estableciendo un único criterio que habilitaría una conservación no individualizada, el criterio geográfico cuando exista un riesgo elevado de preparación o comisión de un delito grave o grave riesgo para la seguridad pública:

Por último, la sentencia del Tribunal De Justicia (Gran Sala), de 6 de octubre de 2020 vuelve a tratar la conservación de datos, concluyendo que, si bien, este tribunal se reafirma en su oposición a medidas legislativas de los Estados miembros que establezcan, para los fines previstos en la Directiva 2002/58, con carácter preventivo, una conservación generalizada e indiferenciada de los datos de tráfico y localización de las comunicaciones, no se opone a otras medidas legislativas que:

> Permitan, a efectos de la protección de la seguridad nacional, recurrir a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas para que procedan a una conservación generalizada e indiferenciada de los datos de tráfico y de localización, en situaciones en las que el Estado miembro en cuestión se enfrenta a una amenaza grave para la seguridad nacional que resulte real y actual o previsible…

Efectivamente, la inteligencia aportada por estos datos no se refiere al contenido de la comunicación, pero no por ello deben

ser minusvalorados. Se trata de metadatos de las comunicaciones y recordemos lo que dijo el exdirector de la NSA y de la CIA Michale Hayden: «We kill people based on metadata» (Krishnan, 2015: 19). No en vano, algunas fuentes indican que la interceptación de las comunicaciones móviles y los metadatos de localización adquiridos por el Ejército ucraniano han sido de gran relevancia para la ejecución de ciertos ataques que acabó con la vida de numerosos oficiales de alto rango rusos que emplearon comunicaciones móviles no cifradas durante los primeros días de la ofensiva rusa en enero y febrero de 2020[10]. Para conocer más sobre procedimientos de explotación geoespacial de este tipo de datos ver *La geolocalización diferida*, de Gómez Gómez (2019).

3.2.4. Interceptación activa de comunicaciones o *end point interception*

La aparición de las tecnologías de cifrado de comunicaciones punto a punto aplicadas a los sistemas comerciales de comunicaciones IP ha supuesto un extraordinario desafío para la eficacia de las capacidades COMINT de los Estados democráticos. Estas soluciones de cifrado hacen prácticamente imposible el acceso no autorizado por el emisor o receptor de la comunicación a su contenido, no siendo esto posible ni siquiera para agencias gubernamentales facultadas para la ejecución de medidas COMINT.

Para solventar esta disfunción, los Estados han accedido a soluciones de interceptación de comunicaciones denominadas *End Point Interception* (EPI) que acuden al punto final o inicial de una comunicación para ser interceptada antes de que tenga lugar su cifrado. Por ejemplo, en caso de la telefonía móvil, estas soluciones, en lugar de interceptar el flujo de la comunicación a través del operador de la red o de manera táctica directamente en la fase radio de la comunicación, canales en los que la cifra ya ha tenido lugar, una solución EPI lleva a cabo el acceso al contenido de la comunicación en el propio terminal móvil del emisor o del receptor, antes o después de que tenga lugar el cifrado o el descifrado, empleando para ello un *software* de control remoto que ha sido instalado en el terminal de manera encubierta y que actúa de la misma forma durante todo el proceso.

Esta figura que, tiempo atrás, podía ser considerada oscura y más propia de actores maliciosos que de Estados democráticos,

[10] Véase: https://www.bbc.com/news/world-europe-60807538 (Tobias, 2022).

es hoy en día una herramienta fundamental al servicio de la ley y de la protección de la Seguridad Nacional. Sin ir más lejos, esta medida está contemplada por la legislación procesal penal española de manera sustantiva, como una medida de investigación tecnológica más al servicio de las autoridades judiciales competentes en la lucha contra el crimen organizado, el terrorismo y la delincuencia grave o a través de Internet. En concreto, la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, en su Capítulo IX, regula los registros remotos sobre equipos informáticos. En su Artículo 588 *septies* a, establece las condiciones y garantías que deben darse para su ejecución.

Herramientas concretas empleadas para este tipo de medidas de investigación han salido tristemente a la palestra de los medios de comunicación social en los últimos tiempos. Un ejemplo es el presunto uso de la de solución israelí de monitorización remota de terminales de comunicaciones móviles inteligentes conocida como PEGASUS para el espionaje de ciertos miembros del Gobierno de España[11] y del de la Generalidad de Cataluña[12].

3.3. Interceptación masiva de comunicaciones

3.3.1. Interceptación masiva a través del *internet back bone*

Para introducir esta técnica COMINT recurriremos a una reciente sentencia del Tribunal Europeo de Derechos Humanos (en adelante TDH) a la que acudiremos en más ocasiones a lo largo de esta investigación. Se trata de la Sentencia de la Gran Sala del TEDH conocida como Caso Big Brother Watch and others v. the United Kingdom (2021). Esta sentencia explica que las comunicaciones vía Internet se realizan principalmente a través de cables de fibra óptica submarinos internacionales operados por los proveedores de servicios de comunicaciones (en adelante CSP). Cada cable puede contener varias portadoras de las 10.000 portadoras que sustentan todo Internet. Tengamos en cuenta que prácticamente todas las comunicaciones electrónicas de hoy en día, incluida la telefonía móvil, circulan por Internet. Una comunica-

[11] Véase: https://www.elmundo.es/espana/2022/05/10/627a3f0fe4d4d8e2258b45a2.html (Peñalosa, 2022).

[12] Véase: https://www.elmundo.es/espana/2022/05/06/62740aecfdddff27338b4587.html (Cruz, 2022).

ción por Internet se divide en paquetes (unidades de datos) que pueden transmitirse por separado a través de una combinación de caminos, generalmente los de mayor rapidez y menor coste. Por lo tanto, algunos o todos los paquetes de una comunicación concreta enviada de una persona a otra, ya sea dentro de un país en especial o a través de sus fronteras, pueden conducirse a través de uno o más países si ese es el camino óptimo para los CSP implicados.

Según esta sentencia, las revelaciones de Edward Snowden realizadas en 2013 indicaban que el Government Communications Headquarters (en adelante GCHQ), que es uno de los servicios de inteligencia del Reino Unido, estaba llevando a cabo una operación, con el nombre TEMPORA, que le permitía intervenir y almacenar volúmenes de datos extraídos de las portadoras mencionadas en el párrafo anterior. Las autoridades del Reino Unido no confirmaron ni desmintieron la existencia de dicha operación, siempre según el TEDH.

Según el TEDH, el GCHQ operó mediante dos procedimientos de interceptación masiva. El primero estuvo dirigido a un pequeño porcentaje de portadoras. Conforme las comunicaciones circulaban a través de las portadoras, eran comparadas con una lista de selectores simples, bien de identidad o de contenido. Si un selector era activado en relación con una comunicación observada, esta era almacenada. Las comunicaciones que no activaban selector alguno eran desechadas. Las comunicaciones almacenadas eran más tarde sometidas a un traje para valorar su interés y, solo en caso de ser valoradas como de alto interés para la inteligencia, eran finalmente abiertas y leídas por analistas. El segundo procedimiento identificado estaba dirigido a un número aún menor de portadoras, seleccionadas por considerarse de gran probabilidad que contuvieran inteligencia de interés. Este segundo sistema contaba con dos fases. En la primera se aplicaban una serie de filtros y reglas para desechar material con menos probabilidad de ser de valor, en la segunda se aplicaban reglas complejas de búsqueda de contenidos de interés para la inteligencia. Estas búsquedas generaban un índice, y los analistas solo podían examinar los elementos que figuraran en él. Todas las comunicaciones que no figuraran en el índice debían ser descartadas.

Podemos comprobar, a la vista de la descripción de este tipo de procedimiento hecha por el TEDH, cómo se trata de sistemas de interceptación propios de servicios de inteligencia y no de autoridades competentes en investigación criminal, que, como hemos

comprobado en los epígrafes anteriores, han de someterse a requisitos más exigentes en lo relativo a restricciones del uso de técnicas COMINT, y especialmente en lo que tiene que ver con la concreción del individuo objeto de la limitación del derecho al secreto de las comunicaciones que se pretende vulnerar.

3.3.2. Interceptación masiva desde plataformas ISR aéreas y aeroespaciales

La característica fundamental de esta capacidad COMINT es el empleo para su despliegue de plataformas aéreas o aeroespaciales estratégicas que permiten vuelos a grandes alturas y con muy altas autonomías. Estas dos prestaciones permiten que los medios técnicos COMINT embarcados, que operan en el espectro radioeléctrico, adquieran alcances de cientos de kilómetros, y que su capacidad de persistencia sobre una zona objetivo sea prácticamente ilimitada. Todo lo anterior, unido a la no necesidad de colaboración por parte de CSP o tercero alguno, hacen que esta sea una capacidad COMINT masiva, a diferencia de la capacidad de interceptación táctica dirigida y pese a que ambas emplean tecnologías de interceptación de análoga naturaleza.

Según Krishnan (2015), en 2013, el Gobierno estadounidense solicitó al fabricante de los drones conocidos como Predator, que incluyeran una capacidad SIGINT[13] para rastrear a los individuos a través de sus teléfonos móviles, así como la capacidad de ubicar mediante radiogoniometría[14] tanto teléfonos móviles como otros transmisores de radiofrecuencia. Según el mencionado autor, la inteligencia de los Estados Unidos ha tenido que descansar en las capacidades SIGINT para localizar individuos de manera global. En este orden de cosas, Currier y Maass (2015) hacen referencia a informes clasificados del Gobierno estadounidense del periodo del presidente Obama, en los que se dan detalles del uso de capacidades SIGINT embarcadas en drones con capacidades estratégicas para su contribución a misiones F3EA[15], en concreto

[13] La disciplina de obtención de inteligencia SIGINT incluye las capacidades ELINT y COMINT.

[14] Esta tecnología puede geolocalizar terminales de comunicaciones inalámbricas con extrema precisión.

[15] La F3EA (Find, Fix, Finish, Exploit & Analyze) se convirtió en doctrina estadounidense en las campañas de contrainsurgencia en Irak y Afganistán a mediados de la década de 2000. El general Stanley McChrystal escribió en sus memorias que la simplicidad de esas «cinco palabras en una línea [...] contradecía la profundidad con que impulsarían nuestra misión». En 2008, Flynn, que trabajó estrechamente con Mc-

durante las campañas de África del Este y Yemen. La monitorización y ubicación precisa de terminales de comunicaciones fue empleada para abatir objetivos de alto valor y para evaluar los efectos de los ataques realizados tras los mismos.

Krishnan (2015) también afirma que cualquier dispositivo inalámbrico puede ser rastreado y que cualquier persona que lo emplee puede ser localizada, al menos aproximadamente, en cualquier parte del mundo utilizando satélites SIGINT de la National Security Agency (en adelante NSA) y sus capacidades cibernéticas. No en vano, este autor afirma que el futuro de la defensa estadounidense consistirá en un sistema de capas verticales que tendrá la mayor parte de sus elementos C2[16] en el espacio, sus elementos clave de vigilancia en la alta estratosfera y la mayor parte de sus capacidades cinéticas en la baja atmósfera.

4. Los conflictos híbridos en la actualidad

4.1. Naturaleza de los conflictos híbridos

La experiencia de los conflictos militares, incluidos los asociados a las llamadas Primaveras Árabes en el norte de África y Oriente Medio, confirma que un Estado completamente próspero, en cuestión de meses e incluso días, puede convertirse en un escenario de feroz lucha armada, en una víctima de la injerencia extranjera, y sumergirse en el abismo del caos, la catástrofe humanitaria y la guerra civil (Gerasimov, 2013).

Según la doctrina para el empleo de las FAS publicada por el Ministerio de Defensa del Gobierno de España (2018), un conflicto aparece cuando varios actores o Estados persiguen objetivos incompatibles entre sí. Los conflictos actuales son más impredecibles, complejos y convulsos que en décadas anteriores. La frontera entre paz y guerra se ha difuminado y no son claros los límites entre seguridad exterior e interior. En esas circunstancias conviven adversarios de difícil identificación y riesgos y amenazas cambiantes, no ya como paso previo al conflicto, sino como conflicto mismo.

Chrystal antes de convertirse en jefe de la Agencia de Inteligencia de Defensa, escribió que «Exploit-Analyze» comienza el ciclo de nuevo, proporcionando pistas, o puntos de partida, en la red que podría ser observada y rastreada utilizando ISR aerotransportado (Currier & Maass, 2015).

16 Mando y control.

En este entorno, la Doctrina para el empleo de las FAS identifica diferentes tipos de adversario, describe sus formas de actuación asimétricas, la amenaza híbrida y una zona dentro del espectro de los conflictos denominada zona gris. Identifica como adversarios no solo los tradicionales, sino también otros actores no estatales que no están sujetos a las mismas regulaciones internacionales que los Estados o las organizaciones internacionales. Es el caso de actores tales como organizaciones terroristas, las organizaciones criminales o las guerrillas o milicias. Es habitual que ciertos grupos de estas naturalezas presenten un comportamiento híbrido entre esas tres naturalezas mencionadas según las circunstancias del momento.

Es común que estos adversarios actúen de una forma asimétrica que les permita explotar al máximo sus capacidades y las vulnerabilidades del contrario. Esta asimetría no se fundamenta tanto en una diferencia de capacidades de combate, sino en las discrepancias morales y las diferencias en los procedimientos empleados respecto de los de los Estados a los que se oponen.

Este escenario constituye un caldo de cultivo ideal para la amenaza híbrida, cuya característica principal, según la Doctrina para el empleo de las FAS, es que trata de alcanzar sus objetivos evitando cruzar el umbral que define el conflicto abierto, evitando la escalada militar[17].

La Estrategia de Seguridad Nacional (2021) publicada por el Gobierno de España establece que:

> Ha aumentado el uso de las estrategias híbridas que, mediante acciones coordinadas y multidimensionales, tratan de explotar las vulnerabilidades de los Estados y sus instituciones con un objetivo de desestabilización o coerción política, social o económica. Estas estrategias se caracterizan por la dificultad de atribuir su autoría y por emplear medios que pueden incluir, además de acciones convencionales, otras como campañas de desinformación, ciberataques, espionaje, subversión social, sabotaje, coacción económica o el uso asimétrico de medios militares (2021: 26).

[17] Según esta doctrina: «La amenaza híbrida se caracteriza por emplear, de forma simultánea y adaptativa, todo tipo de instrumentos de poder; procedimientos convencionales junto a tácticas irregulares y a actividades terroristas; crimen organizado; nuevas tecnologías; ataques en el ciberespacio; presión política y múltiples tipos de herramientas de información y desinformación, incluyendo las noticias falsas y la mentira en sí misma. Todo ello evitando o limitando los enfrentamientos convencionales» (2018: 89).

El Hybrid CoE[18] organizó un seminario en octubre de 2020 denominado «Military Police in Hybrid War» del que se extrajeron las siguientes conclusiones:

> La guerra híbrida explota las vulnerabilidades en las zonas grises de las interfaces del conflicto. Por lo tanto, los actores de la guerra híbrida tienden a operar simultáneamente en múltiples dominios en las sombras de varias interfaces: por ejemplo, entre la guerra y la paz, el amigo y el enemigo, la seguridad interna y externa, los dominios civiles y militares, los actores estatales y no estatales, así como entre el mundo virtual y el real, y entre la realidad y la propaganda.
>
> De este modo, la guerra híbrida difumina las líneas tradicionales de orden y responsabilidades, al tiempo que pretende su posterior disolución con el objetivo último de crear ambigüedades, dificultar la atribución y paralizar el proceso de toma de decisiones del adversario (2020).

La guerra híbrida moderna, a pesar de no ser un fenómeno genuinamente de nuevo cuño, tiene un poder transformador en los cálculos del potencial beligerante de un contendiente. Esto es debido al surgimiento de los actores no estatales, al uso de las tecnologías de la información y a la proliferación de sistemas de armas avanzados (Teífukova y Erol, 2017). El énfasis en los métodos de confrontación utilizados se está desplazando hacia el uso generalizado de medidas políticas, económicas, informativas, humanitarias y otras no militares implementadas con el uso del potencial de movilización reivindicativa de la población. Todo esto se complementa con medidas militares encubiertas, incluyendo la implementación de medidas de confrontación de información y la actuación de fuerzas de operaciones especiales. El uso abierto de la fuerza, a menudo bajo la apariencia de mantenimiento de la paz y gestión de crisis, solo se adopta en algún momento, principalmente para lograr el éxito final en el conflicto (Gerasimov, 2013).

Recientemente, el Parlamento Europeo ha descrito las formas que adoptan las tácticas empleadas por la injerencia extranjera en este ámbito de la guerra híbrida. Estas modalidades representan un gran abanico de acciones, como por ejemplo la desinformación, las amenazas y acoso a periodistas, la captura y cooptación de élites y la instrumentalización de los inmigrantes

[18] The European Centre of Excellence for Countering Hybrid Threats.

y el espionaje, entre otras muchas[19] (INGE Consolidated Draft Report, 2022: 6).

También existe evidencia de que algunos Estados malintencionados y autoritarios, como Rusia, China y otros, utilizan la manipulación de la información y otras tácticas de injerencia para interferir en los procesos democráticos de la UE. Sin duda se trata de parte de una estrategia de guerra híbrida y constituyen una violación del derecho internacional (INGE Consolidated Draft Report, 2022: 6). Según el informe de la Alliance for Secring Democracy emitido en 2020, relativo a la financiación extranjera encubierta, más de 300 millones de dólares fueron inyectados en 33 países durante la última década por parte de Rusia, China y otros regímenes autoritarios con el objeto de interferir en procesos democráticos (INGE Consolidated Draft Report, 2022: 55).

En este sentido, parece necesario en la UE llegar a un acuerdo sobre definiciones y metodologías comunes y granulares para mejorar la compresión común de esta amenaza y desarrollar normas comunitarias adecuadas para mejorar la capacidad de atribución y la respuesta. Así, la UE debería liderar la generación y puesta en marcha de este marco normativo para la atribución de la injerencia extranjera (INGE Consolidated Draft Report, 2022: 7).

4.2. La zona gris

Según la Doctrina para el empleo de las FAS (2018), el adversario en el marco de la amenaza híbrida se comporta de una manera asimétrica en capacidades y forma de operar, rehúye el enfrentamiento allá donde se sabe inferior y lo busca donde explotará mejor sus capacidades y las vulnerabilidades de su oponente.

[19] En concreto se recogen las siguientes modalidades de acciones: la desinformación, la supresión de información, la manipulación de las plataformas de los medios de comunicación social y sus algoritmos, términos y condiciones, y sistemas de publicidad, los ciberataques, las operaciones *hack-and-leak* para acceder a información electoral sobre votantes e interferir en la legitimidad de procesos electorales, las amenazas y acoso a periodistas, investigadores, políticos y miembros de organizaciones de la sociedad civil, las donaciones y préstamos encubiertos a partidos políticos, las campañas a favor de determinados candidatos, organizaciones y medios de comunicación, los medios de comunicación falsos o por delegación, la captura y captación de élites, el dinero «sucio», las personas o identidades falsas, la presión para la autocensura, explotación abusiva de las narrativas históricas, religiosas y culturales, la presión sobre las instituciones educativas y culturales, la toma de control de las infraestructuras críticas, la presión sobre los extranjeros que viven en la UE, la instrumentalización de los inmigrantes y el espionaje.

A veces, empleará actores interpuestos o *proxies*, fuerzas no reconocidas o incluso civiles. Podrá usar formas de actuación alegales o abiertamente ilegales. Mantendrá su identidad y propósito oculto o, incluso, carecerá de un propósito definido, manejando conceptos diferentes de victoria, derrota e importancia del tiempo. Estos actores asimétricos pueden no reconocer autoridad internacional alguna, además de defender principios y valores distintos o antagónicos a los de sus oponentes. Es en las diferencias morales y de procedimientos donde radica el fundamento principal de esta asimetría, en ellas se sustenta su capacidad de obtener ventaja sobre su adversario dificultando en él la adopción de una respuesta adecuada.

La Doctrina para el empleo de las FAS caracteriza la zona gris de la siguiente manera:

> Existe una zona del espectro de los conflictos donde predominan las actuaciones situadas al margen del principio de buena fe entre Estados (*bona fide*) que, pese a alterar notablemente la paz no cruzan los umbrales que permitirían o exigirían una respuesta armada. Es la llamada zona gris.
>
> Los vacíos legales o la normativa excesivamente garantista, las debilidades políticas, sociales, organizativas y de resiliencia de los Estados, la burocratización de la gestión del conflicto y la complejidad en el proceso de toma de decisiones son elementos que conforman la magnitud de la zona gris.
>
> Las actividades que se pueden llevar a cabo en esta zona, entre las que se encuentran ciberataques, la propaganda, los sabotajes, las operaciones encubiertas o clandestinas, los disturbios y otras similares, tienden a mantenerse en un entorno de baja intensidad. Dichas actividades, con mayor o menor grado de ambigüedad y visibilidad, persiguen crear un clima de desinformación y confusión que desestabilicen y debiliten al adversario (2018: 91).

La zona gris se explica *sensu contrario*, es decir: «[…] como un conjunto de actitudes, instrumentos y estrategias que no son ni *White* (paz, de acuerdo con la citada *bona fide*) ni *Black* (guerra abierta, híbrida o convencional)» (Baqués, 2017: 12).

Baqués (2017) considera que la guerra híbrida es tan guerra como la convencional y que, por tanto, quien decide acometerla como medio de alcanzar una situación deseada, asume conscientemente el riesgo de que terceros tomen medidas de represalia amparadas por el Derecho Internacional. En este ámbito, un

Estado que pretende explotar la zona gris de dicho escenario hace uso de la falta de claridad de las normas jurídicas para alcanzar sus objetivos políticos, militares o de otro tipo, antes de que la comunidad internacional pueda juzgar sus acciones como ilegales y tomar medidas para detenerlas (Kleczkowska, 2019). En consecuencia, para Baqués (2017), esto es la zona gris, el modo en el que un actor va a concretar un desafío, sin llegar a la guerra abierta por considerarla excesivamente imprudente, costosa o arriesgada, pero desenvolviéndose fuera de la normalidad de las prácticas internacionales en tiempo de paz.

Es también de reseñar el papel que ciertos actores no estatales pueden desempeñar en la zona gris, bien como *proxis* de otros actores estatales o bien en beneficio de sus propios intereses. Los Estados interesados en generar zonas grises suelen emplear para ello *proxis*, que pueden ser otros Estados, pero también actores no estatales. En el caso de estos actores no estatales, se ha discutido hasta qué punto pueden ser, por sí mismos, los impulsores de una zona gris. No es una hipótesis descabellada, es conveniente analizar el rol de las organizaciones terroristas o grupos insurgentes que aspiran a crear su propio Estado, o de minorías étnicas que pueden movilizarse en el interior de Estados o el caso de las Primaveras Árabes, consideradas por algunos autores como actuaciones en la zona gris por parte de potencias occidentales (Baqués, 2017).

Por su parte, un adversario asimétrico, puede valerse de las ventajas de las técnicas híbridas en la zona gris gracias a su tolerancia moral a infringir el principio de buena fe entre Estados de una forma velada. Si ponemos en conexión esta conclusión con la caracterización de guerra híbrida propuesta por Galeotti: «la ética de la guerra total aplicada hasta a la más pequeña escaramuza» (2016)[20], podemos inferir cómo, en estas circunstancias, el adversario asimétrico planea y conduce sus acciones en clave de guerra, mientras evita que su oponente pueda adoptar medidas oportunas acordes a ese ataque y especialmente a los fines estratégicos de su autor. De esta manera, el actor atacado queda en una situación de vulnerabilidad, incluso indefensión, generalmente por la incapacidad de atribución de las acciones que sufre y por una falta de determinación y agilidad en la toma de decisiones. Tiene lugar, por tanto, una inacción que puede deberse a un sentimiento de ausencia de legitimación moral para actuar

[20] *Vid.* Supra. III.1.

proporcionalmente contra y en consecuencia de una acción que no se identifica como una agresión de guerra por parte del Estado que la sufre, pero que, como hemos visto, sí lo es para el que la ejecuta.

Es preciso, llegados a este punto, mencionar la Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación (2022/2268[INI]). Esta resolución refleja la preocupación de los miembros de la UE por la creciente incidencia y la naturaleza sofisticada de los intentos de injerencia extranjera y de manipulación de información que está sufriendo la propia Unión y sus Estados miembros, principalmente por parte de Rusia y China. En concreto, hace referencia a como Rusia se dedicó a la desinformación con una malicia y una magnitud sin parangón en el período previo a la guerra de agresión contra Ucrania y durante la misma, demostrando que incluso la información puede convertirse en un arma.

A la vista de esta resolución, puede comprobarse cómo los miembros del Parlamento Europeo están preocupados por los muchos vacíos de los que adolecen las políticas y la legislación a nivel Unión Europea y Estados miembros dedicada a la detección, prevención y combate de la injerencia extranjera. En especial, se señala la falta de procedimientos de alerta ante la seriedad de las amenazas actuales procedentes de regímenes autoritarios y otros actores maliciosos, así como la ausencia de estándares suficientes y apropiados y de medidas para identificar y responder ante actos de injerencia extranjera. En consecuencia, esta decisión del Parlamento Europeo llama a la Comisión Europea a proponer una estrategia multicapa, coordinada y multisector, y una adecuada dotación presupuestaria dirigida a equipar a la UE y a sus Estados miembros con adecuadas políticas de previsión y resiliencia y con herramientas de disuasión. Esta estrategia se construirá sobre cuatro pilares: una terminología y definiciones comunes, políticas concretas, capacidades adecuadas de disrupción y defensa y respuesta diplomática y de disuasión.

La estrategia antes mencionada deberá basarse en el análisis de riesgos, y en un enfoque desde el punto de vista de toda la sociedad y todos los Gobiernos.

Por último, el Parlamento Europeo pide a la Comisión que considere, junto con el Servicio Europeo de Acción Exterior, la creación de un Centro europeo para el tratamiento de las injerencias

y la integridad de la información, independiente y con buenos recursos, para identificar, analizar y documentar las operaciones de manipulación de la información y las amenazas de injerencia contra la Unión en su conjunto.

Así, el Parlamento Europeo ha tomado conciencia plena de cómo la injerencia extranjera por parte de regímenes autoritarios u otros actores, puede estar tomando ventaja del uso de ciertas herramientas de influencia ante vacíos legales o incluso disfunciones administrativas, burocráticas o de los procesos de decisión, para obtener ventajas desproporcionadas para sus intereses maliciosos sin la necesidad de escalar a un conflicto abierto, bien híbrido o armado. La batalla en la zona gris ha sido y es una realidad y la UE quiere defenderse y disuadir con medidas efectivas, legales y de otras índoles. Ciertamente, la explosión del conflicto bélico en Ucrania abre un conflicto bélico entre Rusia y este país, pero los países occidentales permanecen en un espectro del conflicto con Rusia alejado, por el momento, del enfrentamiento militar abierto, donde el uso de técnicas de injerencia persiste.

4.3. El crimen organizado en la zona gris

En epígrafes anteriores hemos podido ya atisbar como las estrategias de la guerra híbrida y, en concreto, ciertas acciones ejecutadas en la zona gris del espectro de los conflictos toman ventaja de actividades criminales para generar efectos de gran rentabilidad para alcanzar resultados desproporcionados en la dirección de los objetivos marcados por los actores agresores.

Por ejemplo, las *aktivnye meropriyatiya* (medidas activas), paradigmáticas de la doctrina de la inteligencia rusa, son acciones encubiertas de difícil atribución que buscan influir políticamente, desde la corrupción y la desinformación hasta el asesinato directo e, incluso, el patrocinio de golpes de Estado (Galeotti, 2021a).

Algunos autores ven, en general, en las técnicas híbridas que promueven la subversión social un tipo de corrupción, desde el punto de vista legal, para el que hay que desarrollar los adecuados medios de castigo cuando está ligada a la injerencia extranjera (Tenzer, 2021).

En el caso de este tipo de medidas activas basadas en aspectos económicos, como vemos, especialmente susceptibles de encuadrarse en la zona gris, pueden abarcar desde sanciones hasta subvenciones legales, negación de créditos, concesión de ayu-

das en condiciones especialmente favorables, cortes de suministros energéticos o la manipulación de precios. Estas medidas son especialmente efectivas cuando producen sinergia con otras como la construcción de narrativas sociales o la implicación de organizaciones criminales afines o que compartan intereses. En este ámbito también puede mencionarse el potencial uso de organizaciones no gubernamentales (en adelante ONG) afines para influir en la población o el empleo de ciberataques, mediante cibercriminales estatales o no estatales, para perjudicar el normal desarrollo de la prestación de servicios o suministros, desacreditando la solvencia de Gobiernos objetivo (Baqués, 2017). Por ejemplo, en el caso de Bulgaria, algunos analistas han sugerido que Rusia ha estado implicada en actividades corruptas para expandir el control sobre el mercado de la energía, perjudicando la diversificación y, todo ello, tomando ventaja del apoyo de protestas *anti-fracking* (Cohen and Radin, 2018: 90-91) (Radin *et al*., 2020).

Hemos comprobado cómo el terrorismo y el crimen organizado pueden ser herramientas para la explotación de un conflicto híbrido, especialmente en la zona gris. Por su parte, las organizaciones criminales transnacionales tratan de aprovechar las condiciones favorables que les ofrecen Estados fallidos o espacios de disputa forjando alianzas con funcionarios corruptos o servicios de inteligencia. Se benefician de la desestabilización de instituciones políticas, financieras y de seguridad en Estados frágiles. La acción combinada de crimen organizado y terrorismo tiene efectos devastadores en un Estado frágil, frenando toda opción de crecimiento y desarrollo (Martínez Valera, 2018). Sin duda, se trata de una más que suculenta combinación de herramientas para el alcance de importantes efectos por parte de agresores en la zona gris del espectro de un conflicto, que les permite camuflar su participación en el mismo tras la pantalla de los intereses económicos del crimen organizado y los reivindicativos de las organizaciones terroristas en cualquier situación de precrisis, crisis o poscrisis.

Pero, como hemos comprobado ya, no siempre son Estados los protagonistas de agresiones híbridas en la zona gris. De hecho, en ocasiones son proto-Estados o sub-Estados, como son el caso de Daesh y Hezbollah. Una de las características más importantes que deben poseer estos actores violentos no estatales es la de su independencia económica. Para ello, buscan financiación asociándose, ocasionalmente, con organizaciones criminales transnacionales y utilizando sus métodos. Los países occidenta-

les deben crear una estrategia que constriña el entorno en el que operan estas organizaciones terroristas, atacando no solo a las células operativas, sino también a sus redes de apoyo logístico y financiero (Martínez Valera, 2018).

Es interesante mencionar también que, según Baqués (2017), la amenaza de la actuación de un actor hostil en la zona gris en una dinámica posconflicto armado o poscrisis también ha de ser tenida en cuenta. Tras la victoria militar, no puede darse por sentado que los objetivos han sido cubiertos, pues la situación social, política o económica puede volver a empeorar: «Entrando en una espiral de constante acción-reacción armadas» (p. 16). Con esto, queremos señalar que, tras la finalización de un conflicto armado, la acción hostil en la zona gris puede continuar, y por supuesto en forma de crimen organizado, para socavar la gobernanza, la situación social y la económica, y frustrar así la consolidación definitiva y global de una victoria.

Según Galeotti (2021b), las amenazas no militares son tan importantes como las militares, y es crucial abordar cuestiones que van desde la adecuación de los servicios policiales y de contrainteligencia hasta el reto de la corrupción. Dicho autor, insta a que los países y alianzas analicen de forma aguda y honesta sus vulnerabilidades antes de considerar respuestas institucionales y operativas a las agresiones en la zona gris o de guerra híbrida, pues considera mucho más fácil crear resiliencia de forma preventiva que responder en medio de un ataque.

Por todo lo anterior, es perentorio analizar las vulnerabilidades del Estado de derecho en los países democráticos ante estas amenazas en la zona gris y, en particular, en lo que atañe al objeto de esta investigación, el aprovechamiento que los actores hostiles pueden pretender explotar de las garantías que el marco jurídico en tiempo de paz exige para la protección de los DDFF de los ciudadanos. Al objeto de evitar que estos actores hostiles, cuando injieren en asuntos de un país democrático a través del vector crimen organizado para alcanzar los efectos que pretenden en su beneficio, se aproveche de un marco jurídico de garantías procesales que no permita una acción investigadora contundente contra esas actividades. Por una parte, esta falta de contundencia podría ser consecuencia de una falta de capacidad legal para identificar y atribuir al crimen organizado fines distintos del lucro económico, como serían los de injerencia extranjera en caso de darse. Por otra, por una falta de herramientas o medi-

das de investigación suficientes para contrarrestar dicha acción hostil.

En esta línea, el Parlamento Europeo, en la Resolución Del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación, llama a la Comisión Europea a presentar una propuesta legislativa para adoptar un nuevo régimen de sanciones temáticas para hacer frente a los graves actos de corrupción en el marco de la injerencia extranjera y en la manipulación de información.

5. Derechos fundamentales y garantías jurídicas ante las COMINT

5.1. Derechos fundamentales afectados por las COMINT

En el presente capítulo se pretende enmarcar las técnicas y procedimientos COMINT en el panorama jurídico en general y, para ello, se estudiarán los DDFF a los que afectan, las garantías legales que protegen esos derechos y condicionan los procedimientos de ejecución y las competencias legales de diferentes actores para llevarlos a cabo.

La Declaración Universal de Derechos Humanos (1948) dice en su artículo 12 que: «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección por la ley contra tales injerencias» (Declaración Universal de Derechos Humanos, 1948, Art. 12). Sin duda, los procedimientos COMINT implican injerencias en el derecho fundamental al secreto de las comunicaciones.

Este derecho fundamental al secreto de las comunicaciones ha sido recogido también en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1996, en el artículo 8 del Convenio para la Protección de los Derechos Humanos de las Libertades Fundamentales de 1950, en el artículo 7 de la Carta de Derechos Fundamentales de la Unión Europea de 2007[21], en jurisprudencia

[21] En su artículo 8, el Convenio para la Protección de los Derechos Humanos y las Libertades fundamentales dice:
«Artículo 8. Derecho al respeto a la vida privada y familiar.
1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

del Tribunal Europeo de Derechos Humanos, en el artículo X de la Declaración Americana de los Derechos y Deberes del Hombre de 1948, en el artículo 11.2 y 11.3 de la Convención Americana de Derechos Humanos de 1969 y, en lo que se refiere al ordenamiento jurídico español, en el artículo 18.3 de la Constitución Española (Gómez Gómez, 2019). En concreto, la Constitución Española (1978) dice en su artículo 18.3 que: «Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial».

En cuanto a la relación del derecho al secreto de las comunicaciones y el derecho a la intimidad es interesante apuntar, como hace Gimeno Sendra, que «aun cuando dicho derecho (el de las comunicaciones) claramente se relacione con el derecho fundamental a la intimidad, no se identifica absolutamente con él, sino que posee un contenido mucho más amplio» (Marchal Escalona, 2011: 570).

Una vez visto cómo el Derecho internacional y, en este caso, el Derecho español dan carta de naturaleza al derecho al secreto de las comunicaciones y a su protección, cabe preguntarse qué ocurre en el caso específico del Derecho de los conflictos armados. Los Convenios de Ginebra de 1949 hacen muy pocas referencias a la regulación de la inteligencia, pero la jurisprudencia internacional en este ámbito se ha pronunciado ya profusamente sobre casos en torno a la vigilancia masiva en el extranjero y el derecho a la intimidad, en concreto, lo ha hecho el Comité de Derechos Humanos de la ONU y el Tribunal Europeo de Derechos Humanos[22]. Mediante la aplicación de los principios de legalidad, necesidad, proporcionalidad, garantías adecuadas y acceso a la reparación, estos órganos de supervisión de los tratados han establecido requisitos importantes en relación con la naturaleza, el alcance y los procedimientos que deben cumplir los organismos de inteligencia al llevar a cabo estas operaciones de vigilancia masiva en el extranjero (Lubin, 2022), lo que incluye, lógicamente, la explotación de técnicas COMINT.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás (Convenio Europeo de Derechos Humanos, 1950)».

[22] Centrum För Rättvisa v SwedenApp no35252/08 (19 junio 2018); Big Brother Watch and Others v The United KingdomApp no 58170/13 (13 septiembre 2018); CCPR Concluding Observations: Canada (13 agosto 2015) CCPR/C/CAN/CO/6.

Según Lubin (2022), hay razones de peso para suponer que este cuerpo de jurisprudencia debería seguir vinculando a los Estados incluso durante los conflictos armados por dos razones principales. Primero, si la misma recopilación se lleva a cabo en tiempos de paz, antes del inicio de la guerra, y está sujeta a este estricto marco de DDFF, no hay razones obvias para cambiar las políticas una vez que comienza el conflicto armado. Segundo, como resultado de la guerra global contra el terrorismo, el TEDH ha comenzado a ampliar los límites del derecho a la intimidad en torno a la vigilancia encubierta. La jurisprudencia reciente ha sido deferente con los puntos de vista gubernamentales y se ha acercado a la flexibilización de las restricciones tradicionales.

El TEDH reconoce en una reciente sentencia de su Gran Sala la interceptación masiva de comunicaciones como un recurso de vital importancia para los Estados a la hora de identificar amenazas a su seguridad nacional. En esa misma sentencia se plasma la postura también favorable de los Gobiernos de Francia y de Países Bajos. También apunta en esa dirección la conclusión alcanzada por el Independent Reviwer of Terrorism Legislation que considera esencial la interceptación masiva, primero porque los terroristas, criminales y los servicios de inteligencia hostiles cada vez son más sofisticados evitando la detección por medios tradicionales y, segundo porque la naturaleza de la Internet global implica que la ruta que una comunicación en concreto puede usar para su trasmisión es impredecible (Grand Chamber Case of Big Brother Watch and others v. the United Kingdom, 2021: 128).

Una de las pocas referencias a la vigilancia que podemos encontrar en los Convenios de Ginebra es la contenida en el artículo 92 del Tercer Convenio de Ginebra, que se refiere a los derechos de los prisioneros de guerra y que trata las autorizaciones de vigilancia especial de prisioneros, limitando su uso únicamente a aquellos prisioneros de guerra que habían intentado escapar y habían sido recapturados.

Lubin (2022), basándose en este ejemplo y en el espíritu de los convenios, defiende que: «La introducción de principios limitados del Derecho internacional humanitario, o "salvaguardias", en el contexto de las prácticas de vigilancia masiva en tiempos de guerra es compatible con los objetivos del Derecho internacional humanitario consagrados en los tratados».

Podemos comprobar como el tratamiento de los derechos fundamentales retardativos a la intimidad y, en concreto, al secreto

de las comunicaciones entrañan cierta dificultad cuando se trata de su vigencia en el marco del espectro de un conflicto, tanto en su fase no armada, zona gris, como en la armada. A la dificultad que entraña la velocidad de la evolución tecnológica en sí misma, que está superando la resistencia intelectual y las capacidades normativas de quienes prescriben y aplican las normas del DIH (Lubin, 2022), se puede añadir la confusión entre medios y contenidos privados y propios del combate o de aspectos militares que tienen lugar durante el curso de un conflicto. Hemos podido comprobar durante la invasión rusa de Ucrania cómo mandos y combatientes rusos se han visto obligados a emplear medios no militares (teléfonos móviles convencionales, o transmisores de radiofrecuencia comerciales) para llevar a cabo sus comunicaciones militares, a la vez que hemos comprobado cómo a través de algunos de estos canales se llevan a cabo comunicaciones de interés personal y de interés militar indistintamente[23].

Más allá de lo anterior, también hemos comprobado cómo en los conflictos híbridos y en la zona gris, actores no estatales y estatales se valen de la corrupción, del crimen organizado, del terrorismo o de la subversión para alcanzar sus objetivos. Tanto en tiempo de paz como de guerra este tipo de actividades suelen ser ilícitas y perseguibles por el Estado agredido, haciendo uso de su derecho a injerirse en los derechos fundamentales de los investigados, incluido el derecho al secreto de las comunicaciones.

En el ámbito del Derecho internacional merece ser señalado el caso de las investigaciones por crímenes de guerra, en el marco de las cuales también pueden llevarse a cabo por las autoridades judiciales internacionales investigadoras medidas de investigación que penetren en la esfera de la intimidad y del secreto de las comunicaciones de los investigados[24]. Volviendo al caso de la invasión rusa de Ucrania en 2022, muy probablemente el análisis de inteligencia de datos retenidos asociados a las comunicaciones

[23] Numerosas fuentes resaltan el éxito de Ucrania en la explotación de técnicas COMINT contra las fuerzas rusas durante los primeros meses de la invasión de 2022. En especial a la hora de geolocalizar puesto de mando y militares de alto rango para ser abatidos. Véase *Russian troops' tendency to talk on unsecured lines is proving costly* (Horton y Harris, 2022) o *Russian general Yakov Rezantsev killed in Ukraine* (Tobias, 2022).

[24] Como ejemplo, cabe mencionar la investigación llevada a cabo por el Tribunal Especial para el Líbano, establecido por la ONU para la investigación del homicidio del presidente libanés Rafik Hariri el 14 de febrero de 2005. En dicha investigación fue de gran relevancia el empleo del análisis masivo de los datos conservados asociados a comunicaciones móviles aportados por las compañías operadoras libanesas (Lubin, 2022).

móviles[25] llevadas a cabo en los lugares en los que se produjeron masacres u otros episodios susceptibles de ser investigados como crímenes de guerra, será determinante para la satisfactoria resolución de los casos[26]. Esta técnica, incluyendo la conocida como geolocalización diferida, permitirá, a partir de los datos asociados a las comunicaciones móviles conocidos como CDR (*call data records*), en combinación con el mapeo de las coberturas de telefonía móvil en los lugares de comisión de los crímenes, identificar posibles autores de los hechos y llevar a la confirmación de su participación en los hechos y su ulterior enjuiciamiento[27].

5.2. Garantías jurídicas aplicables

Lubin (2022) considera que no cabe duda de que la recopilación y el análisis de información en tiempo de guerra, incluso con el fin de definir y establecer objetivos, tienen un gran valor. No obstante, dados los daños reales a la privacidad y los posibles abusos derivados de la vigilancia masiva sin restricciones, es igualmente crucial introducir ciertos requisitos de procedimiento y de fondo en el trabajo de la agencia de inteligencia de que se trate en tiempo de guerra como cuestión de derecho internacional vinculante. Así, afirma que los mismos procedimientos adoptados por los organismos de inteligencia, en particular en lo que respecta a las salvaguardias o garantías contra los abusos, deberían persistir. En este sentido, hace referencia a cómo nueva jurisprudencia del TEDH ha reestructurado las salvaguardias que se adoptaron originalmente en el contexto de las investigaciones penales nacionales, para hacerlas más aceptables en relación con las necesidades de las operaciones de vigilancia en el extranjero.

[25] Véase Capítulo II, epígrafe 2.3.

[26] La Corte Penal Internacional ha iniciado una investigación a este respecto, creando un equipo de investigación en el que participarán investigadores españoles de la Guardia Civil. Véase: *Crímenes de guerra en Ucrania: la misión de policías y forenses españoles rastreará vídeos, fotos y vestigios* (Ortega Dolz, 2022).

[27] Esta técnica es la empleada habitualmente en la investigación criminal de homicidios por unidades especializadas como la Unidad Central Operativa de la Guardia Civil, responsable de la resolución, gracias a aquella, de numerosos casos como el asesinato de Diana Quer, Laura Luelmo, el niño Gabriel, o la localización del cuerpo sin vida de Olivia, una de las dos hermanas asesinada por su padre en 2021, entre otros muchos. Este procedimiento consta de cuatro fases: acceso a los datos conservados, tratamiento de estos, mediciones del espectro electromagnético sobre el terreno y análisis de datos (Gómez Gómez, 2019).

En esta dirección, la Gran Sala del TEDH emitió el 25 de mayo de 2021 una sentencia relacionada con los programas de vigilancia sostenidos por los servicios de inteligencia de Estados Unidos y de Reino Unido que fueron filtrados por Edward Snowden. En concreto, la sentencia atañe a la interceptación de comunicaciones llevada a cabo por el Reino Unido y la obtención por su parte de dicha inteligencia vía otros Gobiernos o proveedores de servicios de comunicaciones. Según la documentación filtrada por Snowden, el Goverment Communications Headquarters (GCHQ), uno de los servicios de inteligencia de Reino Unido, realizó una operación llamada TEMPORA, que le permitió interceptar ingentes volúmenes de datos de comunicaciones capturados de las conexiones de Internet por cable de fibra óptica operadas por los proveedores de servicios de comunicaciones.

En lo referente a Estados Unidos, la sentencia de la Gran Sala menciona el programa del Gobierno de los Estados Unidos llamado PRISM, mediante el cual se obtuvo inteligencia de comunicaciones de los proveedores de servicios de Internet. Esta inteligencia fue compartida con el Reino Unido según las filtraciones de Snowden. Otro programa mencionado y ejecutado por los Estados Unidos es el denominado UPSTREAM, orientado a la obtención de contenido de comunicaciones de los cables de fibra óptica e infraestructuras propiedad de proveedores de servicios de comunicaciones estadounidenses. Este programa tuvo amplio acceso a datos globales de ciudadanos no estadounidenses.

Según el contenido de su sentencia, el TEDH ve la interceptación masiva como un proceso gradual en el que el grado de injerencia en los derechos individuales del artículo 8 de la CEDH se incrementa a medida que el proceso avanza. En concreto, el TEDH identifica cuatro fases en el proceso de interceptación masiva:

a) La interceptación y la retención inicial de comunicaciones y datos asociados a la comunicación.

b) La aplicación de selectores específicos sobre la información.

c) El análisis de las informaciones seleccionadas.

d) La subsecuente del dato y el uso del «producto final», incluido el intercambio del dato con terceras partes. (Grand Chamber Case of Big Brother Watch and others v. the United Kingdom, 2021: 98)

La Gran Sala considera que los derechos contemplados en el artículo 8 están afectados en todos y cada uno de los pasos descritos

más arriba. Mientras que la interceptación inicial seguida del descarte de parte de la información no implica una interferencia significativa, el grado de injerencia en los derechos individuales de este artículo incrementa a medida que el proceso de interceptación masiva avanza. El hecho de que los datos almacenados estén cifrados y no puedan ser interpretados sin ayuda de sofisticadas herramientas y su acceso esté restringido a un número limitado de personas no influye para el tribunal en dicha conclusión. Es en la fase final del proceso, cuando la información atribuible a una persona concreta es analizada o un analista examina el contenido de las comunicaciones cuando la necesidad de garantías es la más alta (Grand Chamber Case of Big Brother Watch and others v. the United Kingdom, 2021, 99).

En relación con la interceptación de comunicaciones no masiva o selectiva, denominada *targeted inercetption* en inglés, que es la habitual en investigación criminal, la Gran Sala establece seis garantías mínimas que deben ser claramente definidas en la legislación nacional de los Estados a fin de evitar abusos de poder. Estas garantías mínimas atañen a la naturaleza de las infracciones que pueden justificar la ejecución de la medida, a la definición de las categorías de individuos susceptibles de ver interceptadas sus comunicaciones, al límite de la duración de la interceptación, al procedimiento seguido para el examen, uso y almacenamiento de los datos obtenidos, a las precauciones a adoptar cuando se comunica la información a otras partes y a las circunstancias en las que los datos almacenados deben ser borrados o destruidos. La Corte defiende que estas garantías son menos relevantes en el contexto de la interceptación masiva por motivos de seguridad nacional, cuyo propósito es principalmente preventivo y no el de investigar un objetivo específico y/o una infracción criminal concreta. Sin embargo, para el tribunal es imperativo que, cuando un Estado pretenda explotar una medida de interceptación masiva, la legislación nacional deberá contener normas detalladas sobre cuándo las autoridades pueden recurrir a ella. Por ello, considera que sí son pertinentes en la interceptación masiva cuatro de las seis medidas aplicables a la interceptación selectiva, que son: la fijación en la legislación nacional del límite de duración de la medida; el procedimiento a seguir para el examen, uso y almacenamiento de los datos obtenidos; las precauciones a adoptar cuando se comunica la información a otras partes; y las circunstancias en las que los datos interceptados pueden o deben ser borrados o destruidos (Grand Chamber Case of Big Brother Watch and others v. the United Kingdom, 2021: 105).

En la reciente Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación, se hace especial hincapié en que cualquier acción contra la injerencia extranjera o la manipulación de la información por parte de actores hostiles debe prestar particular atención a su impacto en los DDFF y en las libertades de los ciudadanos de cualquier sanción que se imponga, a fin de mantener el respeto a la Carta de Derechos Fundamentales. Podemos interpretar que dichas garantías habrán de observarse, del mismo modo, a la hora de aplicar cualquier medida de investigación durante el proceso de indagación previo a la imposición de sanciones que pueda contemplarse en los procesos que la UE está impulsando para reforzar su resiliencia ante la injerencia extranjera.

5.3. Competencias para la ejecución de COMINT en la zona gris

A la hora de analizar los organismos competentes para la ejecución de medidas de inteligencia COMINT hemos de distinguir el escenario jurídico en el que nos encontremos. Lógicamente, no será lo mismo encontrarnos en un escenario de precrisis, poscrisis o de crisis no bélico, en el que incluiremos la zona gris, que en un escenario de conflicto armado abierto.

En el primero de los casos, habremos de referirnos a la legislación nacional en vigor, en caso de existir, para determinar los actores competentes para ejecutar medidas COMINT. En lo que se refiere a la interceptación selectiva en ámbito de la investigación criminal en España, habremos de recurrir a la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, y en lo que se refiere a interceptación de comunicaciones por motivos de seguridad nacional recurriremos a la Ley Orgánica 2/2002, de 6 de mayo, Reguladora Del Control Judicial Previo Del Centro de Inteligencia.

La Ley Orgánica 13/2015 regula, entre otras, las medidas de investigación tecnología de interceptación de comunicaciones telefónicas y telemáticas en el ámbito de Derecho procesal penal en su capítulo IV, establece los requisitos de autorización judicial previa dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad. Esta medida podrá ser solicitada a la autoridad judicial por el

Ministerio Fiscal o por la Policía Judicial y será ejecutada por esta última, entre otros motivos, por contar con las capacidades necesarias para ello.

Por su parte, la Ley Orgánica 2/2002 establece en el apartado 1 de su artículo único:

> El secretario de Estado director del Centro Nacional de Inteligencia deberá solicitar al magistrado del Tribunal Supremo competente, conforme a la Ley Orgánica del Poder Judicial, autorización para la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, siempre que tales medidas resulten necesarias para el cumplimiento de las funciones asignadas al Centro[28].

Según Baqués (2017), dado que la zona gris opera en una etapa de paz formal, es habitual que la sociedad civil sea empleada como un inmenso escudo humano y que las garantías constitucionales democráticas tiendan a complicar los diagnósticos, a retrasar las respuestas y a burocratizar la gestión de los conflictos. Como hemos podido ver hasta ahora en el presente capítulo, las garantías legales que deben observarse para la interceptación de comunicaciones en ausencia de conflicto bélico son muy elevadas en un sistema democrático consolidado. Ello se puede constituir en un escudo legal empleado por injerencias extranjeras que traten de sacar partido de actuaciones en forma de crimen organizado, corrupción, terrorismo u otros de los vectores de ataque que puede encuadrarse en la zona gris de los conflictos. Es fundamental entender que, según el mismo autor, un Estado o actor no estatal que agrede en la zona gris a otro no se aplica a sí mismo ni a sus actuaciones la observancia de garantías legales análogas por las que rige su comportamiento. Esto le garantiza una posición de ventaja de extraordinario valor que tratará de explotar al máximo.

Otra debilidad que Baqués (2017) reseña es la falta de cooperación entre departamentos, ministerios o servicios de inteligencia dentro de un mismo Estado, algo a lo que los agresores no son

[28] Estas funciones son asignadas al Centro Nacional de Inteligencia por la Ley 11/2002, de 6 de mayo, Reguladora del Centro Nacional de Inteligencia que en su Artículo 1 dice: «El Centro Nacional de Inteligencia es el Organismo público responsable de facilitar al presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones».

ajenos y que tratarán de explotar en su beneficio. Pongamos un ejemplo, en el marco de una investigación procesal por corrupción en la que una unidad de Policía Judicial investiga bajo la autoridad de un juzgado de instrucción una trama de políticos corruptos facilitadores de concesiones contractuales a empresas de origen ruso a cambio de comisiones ilegales, las actuaciones de investigación y los datos recabados, en muchos casos fruto de la explotación de medidas COMINT, suelen estar sujetos a secreto sumarial.

Claramente, cuando un actor hostil activa la zona gris trata de explotar estas ventajas jurídicas y organizativas que se le ofrecen en la mayor medida posible, evitando cruzar el umbral de la guerra abierta. Este umbral viene determinado por el Derecho Internacional Público, en especial la Carta de Naciones Unidas, pero también por la experiencia acumulada y la práctica estatal, dice Baqués (2017). En relación con la resolución de esta amenaza, concluye este autor que:

> Los desafíos planteados por la zona gris requerirán, con toda seguridad, una nueva teoría del conflicto que sea capaz de integrar en un *continuum* la propia zona gris, la guerra híbrida y la guerra convencional, contando con sus solapamientos y con sus intersecciones, llegado el caso (p. 11).

De todo lo anterior puede deducirse que el marco jurídico de las garantías constitucionales y del Derecho internacional público aplicable a la explotación de COMINT deberá también adaptarse a esa nueva teoría del conflicto que, sin duda, habrá de aprender de la propia amenaza y devenir tan flexible, versátil y ágil como ella misma, permitiendo una detección e identificación temprana de la amenaza y su inmediata neutralización sobre la base de la cooperación interdepartamental e internacional.

¿Quiere decir esto último que la solución para contrarrestar la zona gris exige un marco jurídico propio, a medio camino entre el marco jurídico en tiempo de paz y el Derecho de la Guerra? En cualquier caso, parece razonable considerar que el Derecho en tiempo de paz, y las garantías jurídicas que protegen los DDFF, requieren adaptarse a esta nueva variedad de amenaza para evitar que un Estado democrático se vea obligado a permanecer en una situación vulnerable ante un actor hostil que opera en contra de sus intereses en el espectro de la zona gris. Una forma de llevar esto a cabo es tipificar como delito nuevos patrones de com-

portamiento[29] y regular capacidades especiales de compartición de inteligencia entre agencias, por ejemplo.

Según Tenzer (2021), la capacidad de los Estados de descubrir y atribuir las acciones que caen bajo el paraguas de las agresiones híbridas es el fundamento más esencial de la lucha contra estos ataques. Para este autor, muchos países todavía sufren una dispersión de los servicios encargados de contrarrestar estas amenazas, en particular en su aspecto de corrupción, y sistemas legales con muchas lagunas. En relación con los enlaces entre la corrupción y la inferencia extranjera, Tenzer (2021) hace dos recomendaciones. Primero, emplear grupos de trabajo conjuntos que reúnan a los servicios de inteligencia internos y externos, a la Policía y a los servicios aduaneros y fiscales para identificar a las personas que trabajan para una potencia extranjera; y, segundo, adaptar el arsenal legislativo a la nueva amenaza.

En esta búsqueda de soluciones y de adaptación a las amenazas híbridas, el Parlamento Europeo, en su Resolución de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación, señala la necesidad de una cooperación global y multilateral entre países de ideas afines en los foros internacionales pertinentes, en forma de una asociación basada en un entendimiento común y en definiciones compartidas, con vistas a establecer normas y principios internacionales. Estas definiciones compartidas, bien podrían referirse a tipos delictivos como los referidos anteriormente.

En esa misma resolución, el Parlamento Europeo pide a la UE que defina lo que puede entenderse como un hecho internacionalmente ilícito desde el enfoque de la injerencia extranjera y que adopte los umbrales mínimos para la activación de contramedidas como resultado de esta nueva definición. Y pide igualmente que dicha activación de contramedidas vaya acompañada de una evaluación de impacto para proporcionar seguridad jurídica a las actuaciones. Propone el Parlamento Europeo que los Estados

[29] En esta dirección, la Resolución del Parlamento Europeo, de 9 de Marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación hace referencia a cómo Australia ha modificado su National Security Legislation al objeto de tipificar como delito las actividades encubiertas y engañosas de actores extranjeros que pretendan interferir en procesos políticos o gubernamentales, afectar a los derechos o deberes, o apoyar actividades de inteligencia de un Gobierno extranjero, mediante la creación de nuevos delitos como el de «injerencia extranjera intencionada (intentional foreign interference)».

miembros consideren el establecimiento de un sistema de registro de influencias extranjeras y la creación de un registro de las actividades declaradas realizadas para un Estado extranjero o en su nombre, gestionado por el Gobierno.

Sin duda que el desarrollo de este nuevo escenario jurídico con nuevas herramientas para la neutralización de acciones hostiles no bélicas e híbridas contemplará nuevas tipologías delictivas relacionadas con el crimen organizado y la corrupción, lo que hará posible combatirlas desde la acción penal y policial de manera temprana y contundente, empleando para ello medidas de investigación COMINT.

6. Conclusiones

En definitiva, consideramos que las capacidades COMINT empleadas en la lucha contra el crimen organizado en cualquiera de los espectros del conflicto, tienen una repercusión directa también en la consecución de los objetivos militares que se establezcan en un conflicto en su fase bélica, llegado el caso de que esta se materialice.

El derecho al secreto de las comunicaciones queda protegido por un gran abanico de normativas nacionales; y, sobre todo, del Derecho internacional, habiendo sido ratificado también por jurisprudencia de los más altos tribunales de ambos ámbitos. Esta alta protección está fundamentada en el uso privado de las comunicaciones por parte de los individuos, un uso relativo a su vida privada y familiar (Art. 8 Convenio Europeo de Derechos Humanos, 1950), y en la expectativa de privacidad que albergan para estos asuntos cuando los tratan por dicho medio de comunicación. Si bien es cierto que el uso relativo a la vida privada y familiar de medios de comunicación de sistemas de mando y control militar por parte de unidades desplegadas en un conflicto bélico sería discutible, no lo es en caso de actores como el crimen organizado, en especial cuando actúan en el espectro no bélico del conflicto, como es la zona gris, y pese a que lo haga como vector de injerencia o *proxi* de un actor estatal hostil.

Se pone de manifiesto una falta de preparación generalizada en los actores nacionales e internacionales a nivel europeo para hacer frente a la amenaza híbrida. De ello se hace eco la reciente resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación. Se constata una falta

de aprovechamiento de las capacidades COMINT para identificar y neutralizar la amenaza híbrida cuando progresa empleando el crimen organizado como *proxi*. Esta faceta del crimen organizado, que implica una amenaza a bienes jurídicos superiores, como son la seguridad nacional, más allá de la protección del patrimonio, o la salud pública, por ejemplo, no encuentra un reflejo proporcional en la modulación de las garantías jurídicas que protegen el derecho fundamental al secreto de las compunciones en escenarios de paz formal. Esto es una vulnerabilidad que los actores hostiles explotan y explotarán.

Por todo lo anterior, es perentorio analizar las vulnerabilidades del Estado de derecho en los países democráticos a fin de evitar que actores hostiles, injiriendo en los asuntos de un país democrático a través del vector crimen organizado, se aprovechen de un marco jurídico de garantías procesales que no permita una acción investigadora contundente contra esas actividades.

Es oportuno que los Estados democráticos acometan las siguientes acciones a fin de protegerse ante las amenazas híbridas por medio del aprovechamiento de capacidades COMINT:

- Analizar de forma graduada y honesta el empleo de sus capacidades COMINT antes de considerar respuestas institucionales y operativas contra el crimen organizado en la zona gris o de guerra híbrida.
- Contribuir al desarrollo internacional de una nueva teoría del conflicto, fruto de una asociación de los Estados democráticos basada en un entendimiento común y en definiciones compartidas, con vistas a establecer normas y principios internacionales comunes relativos a la amenaza híbrida (resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación). Para ello, serán necesario definir lo que puede entenderse como un hecho internacionalmente ilícito desde el enfoque de la injerencia extranjera y los umbrales mínimos para la activación de contramedidas. Así, habrán de establecerse estándares suficientes y apropiados de procedimientos de alerta, y de medidas para identificar y responder ante actos de injerencia (resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación). Se propone, como indica el Parlamento Europeo, el establecimiento de un registro de injerencias extranjeras y la creación de un regis-

tro de las actividades declaradas realizadas para un Estado extranjero o en su nombre, gestionado por los Gobiernos. Y todo ello, habrá de hacerse teniendo presente que esta nueva teoría y su desarrollo, siguiendo la línea de Baqués (2017), ha de ser «capaz de integrar en un *continuum* la propia zona gris, la guerra híbrida y la guerra convencional, contando con sus solapamientos y con sus intersecciones, llegado el caso» (p.11). Como dice Tenzer (2021), será fundamental que la nueva teoría y su desarrollo permita descubrir y atribuir acciones, en este caso del crimen organizado, que caigan bajo el paraguas de las agresiones híbridas, lo que es el fundamento más esencial para la lucha contra estos ataques.

- Promover los cambios legales y la adaptación de las garantías legales aplicables a la lucha contra el crimen organizado, tanto en zona gris como en tiempo de conflicto armado, cuando actúa en beneficio de la injerencia extranjera. Remover las limitaciones legales que impidan la compartición eficiente de información entre agencias de información o inteligencia. Tipificar como nuevos delitos ciertas actividades vinculadas al crimen organizado y la corrupción cuando respondan a injerencias extranjeras. Siguiendo a Tenzer (2021), también se propone desarrollar medios de castigo adecuados para el crimen organizado, cuando contribuye a la consecución de objetivos de esta naturaleza en línea con las propuestas del Parlamento Europeo (resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación). En este sentido, recalcamos que ya existen interpretaciones legales en las que se relajan las garantías jurídicas del secreto de las comunicaciones cuando afecta a bienes jurídicos como la seguridad nacional (véase la Sentencia del Tribunal De Justicia [Gran Sala], de 6 de octubre de 2020, en la que se habilita la conservación masiva de datos CDR en caso de afectación a la seguridad nacional de un Estado).
- Plantear cambios organizativos y la adecuación de servicios policiales y de contrainteligencia. Impulsar la cooperación en inteligencia a nivel global y multilateral (resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación). Mitigar la falta de cooperación entre departamentos señalada por Baqués (2017), creando grupos de trabajo conjuntos que reúnan servicios de

inteligencia internos y externos, a la policía y a los servicios aduaneros y fiscales para identificar a las personas que trabajan para una potencia extranjera en línea con la propuesta de Tenzer (2021), en este caso enfocándolos a la explotación conjunta de capacidades COMINT.

- Afrontar el estudio de la explotación de las capacidades COMINT en la lucha contra el crimen organizado en la zona gris no solo en una dinámica precrisis, sino también de crisis y de poscrisis, en línea con lo propuesto por Baqués (2017).

Referencias bibliográficas

1. Textos doctrinales y legales

Convenio Europeo de Derechos Humanos (1950). Disponible en: http://www.echr.coe.int/Documents/Convention_SPA.pdf

Convenio Sobre la Ciberdelincuencia (2001).

Constitución Española (1978). *Boletín Oficial del Estado.*

Declaración universal de Derechos Humanos (1948).

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Pub. L. N.º 2002/58/CE (2002). Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF

Doctrina para el empleo de las FAS. Pub. L. N.º PDC-01(A) (2018). Disponible en: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2018/PDC-01_A_Doctrina_empleo_FAS_27feb2018.pdf

España. (2002). Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. En: *Boletín Oficial del Estado*.

España. (2002). Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia. En: *Boletín Oficial del Estado 16439*.

España. (2007). Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. En: *Boletín Oficial Del Estado*. 261, 19 de octubre, 42617-42623. Disponible en: https://www.boe.es/boe/dias/2007/10/19/pdfs/A42517-42523.pdf

España. (2015). Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. En: *Boletín Oficial Del Estado*. 239, de 6 de octubre, 90192-90218.

España. (2002). Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia. En: *Boletín Oficial del Estado.* 16439.

Estrategia de Seguridad Nacional. (2021).

ETSI. (2009). Lawful interception (LI); retained data handling; handover interface for the request and delivery of retained data (Patent No. ETSI TS 102 657 V1.4.1 (2009-12)).

Grand Chamber Case of Big Brother Watch and others v. the United Kingdom. (May 21, 2021).

Real Decreto 424/2005, de 15 de abril, por el que se aprueba la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios. *Boletín Oficial del Estado* (2005).

Reglamento (UE) 2016/ 679 del Parlamento Europeo y del Consejo –de 27 de abril de 2016– relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/ 46/ CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea* (2016).

Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación. Pub. L. N.º 2020/2268(INI). Disponible en: https://www.europarl.europa.eu/ (2022).

Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 21 de diciembre de 2016, (2016).

Sentencia del Tribunal Europeo de Derechos Humanos sobre el caso Malone contra el Reino Unido, (1984).

STS 279/2017. (19 de abril de 2017). Disponible en: https://vlex.es/vid/678678197

2. Libros, artículos y revistas

Arista, L. (2022, January 19). El crimen organizado intensifica su amago a los Gobiernos al iniciar 2022. En: *Expansión*. Disponible en: https://politica.expansion.mx/mexico/2022/01/19/crimen-organizado-sube-amago-gobiernos-estatales-2022

Aznar Fernández-Montesinos, F. (2021). Fragilidad institucional y delincuencia organizada. El caso de América Central y México. *Bie3: Boletín IEEE, ISSN-e 2530-125X. N.º 22, 2021, pp. 41-59*, *22*, 41–59. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8153016&info=resumen&idioma=ENG

Baqués, J. (2017). Hacia una definición del concepto «Gray Zone» (GZ). *Instituto Español de Estudios Estratégicos*.

Blank, S. (2018). *Moscow's Competitive Strategy*.

Cedeira, B. (2022, January 29). Soldados españoles, en la frontera con Rusia: «Usan drones para hackearnos las torres de telefonía. En: *El Español*. Disponible en: https://www.elespanol.com/espana/20220129/soldados-espanoles-frontera-rusia-usan-hackearnos-telefonia/645935817_0.html

Chekinov, S. G. y Bogdanov, S. A. (2013). The Nature and Content of a New-Generation War. En: *Military Thought*. 10, pp. 12-23. https://www.usni.org/sites/default/files/inline-files/Chekinov-Bogdanov%20Miltary%20Thought%202013.pdf

Cohen, R. S. y Radin, A. (2019). Russia's Hostile Measures in Europe: Understanding the Threat. Disponible en: https://doi.org/10.7249/RR1793

Cruz, M. (2022, May 6). El Gobierno de Sánchez espió a Aragonés por ser una «amenaza» para el Estado. En: *El Mundo* . Disponible en: https://www.elmundo.es/espana/2022/05/06/62740aecfdddff27338b4587.html

Currier, C. y Maass, P. (2015, October 15). Firing Blind: Critical intelligence failures and the limits of drone technology. En: *The Intercept*. Disponible en: https://theintercept.com/drone-papers/firing-blind/

Dubovitski, N. (2014). Sin cielo. En: *Русский Пионер*. Disponible en: http://ruspioner.ru/honest/m/single/4131

Dulles, A. W. (2006). *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World*. 304.

EUROPOL (2021). *Serious and Organised Crime Threat Assessment*. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf

Fowler, M. (2011). Mexico: a Case of Hybrid Warfare. In R. Tomes, P. Brister, y T. Schiller (eds.). *Hybrid Warfare: Transnational Threats and Policy Choices for an Era of Persistent Conflict*.

Center for Emerging National Security Affairs. Disponible en: https://www.academia.edu/12251948/Mexico_a_Case_of_Hybrid_Warfare

Fracchia Figueiredo, M. (2021). El proceso de exterminio selectivo de los activistas sociales en México (enero 2017-abril 2019). En: *Revista de Cultura de Paz*, *5*. Disponible en: http://revistadeculturadepaz.com

Front-line Intelligence - Stedman Chandler. Google Libros. (n.d.). Retrieved December 30, 2021. Disponible en: https://books.google.es/books?id=s8YlPzrQqSgC&pg=PA3&lpg=PA3&dq=Front+Line+Intelligence+by+COL+Robert+Robb&source=bl&ots=8i6wDokNof&sig=ACfU3U1Lb9Z4_srsV93L-zQNFJIlIw2NzQ&hl=es&sa=X&ved=2ahUKEwi-79u7Fnor1AhVH1xoKHWXMDA0Q6AF6BAgNEAM#v=onepage&q=Front%20Line%20Intelligence%20by%20COL%20Robert%20Robb&f=false

Galeotti, M. (2016). *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right: Mayak Intelligence*.

Galeotti, M. (2017). *Crimintern: How the Kremlin uses Russia's criminal networks in Europe*. Disponible en: https://ecfr.eu/wp-content/uploads/ECFR208_-_CRIMINTERM_-_HOW_RUSSIAN_ORGANISED_CRIME_OPERATES_IN_EUROPE02.pdf

Galeotti, M. (2021a). Active Measures: Russia's Covert Global Reach. En: Herd, G. P. (ed.), *Russia's global reach: A security and statcraft assessment,* pp. 118-127. Disponible en: https://www.marshallcenter.org/sites/default/files/files/2021-06/RGR%20Chapter%2014.pdf

Galeotti, M. (2021b). Thinking about hybrid war and the «imagination race. En: *GLOBSEC*. Disponible en: https://www.globsec.org/publications/thinking-about-hybrid-war-and-the-imagination-race3/

García Ferrer, G. (2021, January). Apoyo de las Fuerzas Armadas a las autoridades civiles en los nuevos escenarios: Desafíos en la Zona Gris. En: *Revista Española de Defensa*, pp. 48-49. Disponible en: https://www.defensa.gob.es/Galerias/gabinete/red/2021/01/informe-zona-gris-red-379.pdf

George, R. Z. y Bruce, J. B. (2008). *Analyzing intelligence: origins, obstacles, and innovations*. GeGorgetown University. Center for Peace and Security Studies. Disponible en: https://pdfroom.com/books/analyzing-intelligence-origins-obstacles-and-innovations/0K2ll3LD2ap

Gerasimov, V. (2013, February 27). El valor de la ciencia en la prospectiva. *Военно-Промышленный Курьер*. Disponible en: https://vpk-news.ru/articles/14632

Gill, P. y Phythian, M. (2018). *Intelligence in an insecure world*. Disponible en: https://www.wiley.com/en-us/Intelligence+in+An+Insecure+World%2C+3rd+Edition-p-9781509525195

Gómez Gómez, J. de D. (2019). La geolocalización diferida. En: *Los medios técnicos e investigación criminal*, pp. 119-153. Delta Publicaciones.

Gragido, W. y Pirc, J. (2011). *Cyber Crime and Espionage An Analysis of Subversive Multi-Vector Threats*. 1 online resource, p. 270. Disponible en: http://www.herts.eblib.com/patron/FullRecord.aspx?p=645033 y http://www.studynet.herts.ac.uk/go/accessroute/1

Hoffman, F. G. (2007). *The Rise of Hybrid Wars*. Disponible en: http://www.potomacinstitute.org/

Hollywood, J. S. *et al*. (2018). Emerging Technology Trends and Their Impact on Criminal Justice. Disponible en: https://doi.org/10.7249/RB9996

Horton, A. y Harris, S. (2022, March 27). *Russian troops' tendency to talk on unsecured lines is proving costly*. En: *The Washington Post*. Disponible en: https://www.washingtonpost.com/national-security/2022/03/27/russian-military-unsecured-communications/

Hybrid CoE contributes to NATO Military Police Centre of Excellence webinar on 'Military police in hybrid war' - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats. (n.d.). Retrieved March 12, 2022. Disponible en: https://www.hybridcoe.fi/news/hybrid-coe-contributes-to-nato-military-police-centre-of-excellence-webinar-on-military-police-in-hybrid-war/

INGE Consolidated Draft Report. (2022).

Johnson, L. K. (2007). *Handbook of intelligence studies*. Routledge. Disponible en: http://www.marcialpons.es/libros/handbook-of-intelligence-studies/9780415777834/

Keegan, J. (2003). *Intelligence in war: knowledge of the enemy from Napoleon to al-Qaeda*. 387. Disponible en: https://www.goodreads.com/work/best_book/53815-intelligence-in-war-knowledge-of-the-enemy-from-napoleon-to-al-qaeda

Kent, Sherman. (1965). *Strategic intelligence for American world policy.* Disponible en: https://archive.org/details/in.ernet.dli.2015.86810/page/n29/mode/2up?view=theater

Kleczkowska, A. (2019). Explaining the meaning of «Grey Zones» in public international law based on the example of the conflict in Ukraine. En: *Contemporary Central & East European Law*. 1(133), pp. 75-93. Disponible en: https://doi.org/10.37232/cceel.2019.07

Krishnan, A. (2015). Mass Surveillance, Drones, and Unconventional Warfare. En: *BEHEMOTH A Journal on Civilisation.* 8(2). Disponible en: https://doi.org/10.6094/behemoth.2015.8.2.867

Lárraga, F. S. (2022). Las desapariciones forzadas. En: *Revista Mexicana de Ciencias Penales*. 5(16), pp. 115-142. Disponible en: https://revistaciencias.inacipe.gob.mx/index.php/02/article/view/501

López Obrador, A. M. (2018). *Plan Nacional de Paz y Seguridad 2018-2024*.

Lowenthal, M. M. (2003). *Intelligence: from secrets to policy*, 274.

Lubin, A. (2022). The rights to privacy and data protection under international law and Human Rights law. En: *Research Handbook on Human Rights and Humanitarian Law Further Reflections and Perspectives*. Edward Elgar. Disponible en: https://www.icrc.org/en/document/speech-icrc-president-rules-warthing-past

Mansoor, P. R. (2012). *Introduction: Hybrid warfare in history. Fighting Complex Opponents from the Ancient World to the Present*, pp. 1-17. Disponible en: https://doi.org/10.1017/CBO9781139199254.001

Marchal Escalona, N. (2011). *Manual de lucha contra la droga*. 1100.

Marín Gutiérrez, F. (2022). ¿Comprendemos la desinformación?: Rusia y la evolución de las medidas activas. *IEEE*. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0236&from=PL

Martínez Valera, G. (2018). Actores no estatales en la zona gris. Las organizaciones de carácter violento y crimen organizado transnacional. En: *Boletín IEEE*. 12, pp. 1059-1088. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6959991&info=resumen&idioma=ENG

Oficina de las Naciones Unidas contra la Droga y el Delito. (2020). *UNODC Strategy 2021-2025*. Disponible en: https://www.unodc.org/unodc/es/strategy/full-strategy.html

Ortega Dolz, P. (2022, April 30). Crímenes de guerra en Ucrania: la misión de policías y forenses españoles rastreará vídeos, fotos y vestigios. En: *El País.* Disponible en: https://elpais.com/internacional/2022-04-30/crimenes-de-guerra-en-ucrania-la-mision-de-policias-y-forenses-espanoles-rastreara-videos-fotos-y-vestigios.html

Peñalosa, G. (2022, May 10). El móvil de Marlaska fue espiado con Pegasus en junio y el ministro de Agricultura fue víctima de un hackeo frustrado. En: *El Mundo*. Disponible en: https://www.elmundo.es/espana/2022/05/10/627a3f0fe4d4d8e2258b45a2.html

Porche, I. R. *et al*. (2017). Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below. Disponible en: https://doi.org/10.7249/RR1600

Presidencia de la República. (2021). *Tercer Informe de Gobierno*. Disponible en: https://presidente.gob.mx/wp-content/uploads/2021/09/TERCER-INFORME-DE-GOBIERNO-PRESIDENTE-AMLO-01-09-21.pdf

Rabasa, A., Arroyo Center y Rand Corporation. (2017). *Counternetwork: countering the expansion of transnational criminal networks*. Disponible en: https://books.google.com/books/about/Counternetwork.html?hl=es&id=18NLDgAAQBAJ

Radin, A., Demus, A. y Marcinek, K. (2020). Understanding Russian Subversion: Patterns, Threats, and Responses. Disponible en:. https://doi.org/10.7249/PE331

Reyes, Ó. (2021, June 23). Violencia en Guanajuato sería por disputa entre Cártel de Sinaloa y CJNG. En: *El Sol de México*. Disponible en: https://www.elsoldemexico.com.mx/republica/sociedad/violencia-en-guanajuato-seria-por-disputa-entre-cartel-de-sinaloa-y-cjng-6877552.html

Shulsky, A. N. y Schmitt, G. J. (2002). *Silent warfare: understanding the world of intelligence*. 247.

Teífukova, R. y Erol, M. S. (2017). Russian hybrid war: from theory to practice. En: *ANKASAM Revista Internacional de Crisis y Estudios Políticos. Edición Especial de Hybrid Wars.* 1(2), pp. 33-67.

Tenzer, N. (2021). Countering hybrid threats between common resistance and legal measures. En: *GLOBSEC*. Disponible en: https://www.globsec.org/publications/countering-hybrid-threats-between-common-resistance-and-legal-measures/

Tobias, B. (2022, March 26). Russian general Yakov Rezantsev killed in Ukraine. En: *BBC*. Disponible en: https://www.bbc.com/news/world-europe-60807538

Toedte, B. (2021, June 21). Mexico mid-terms marred by threats, attacks and killings. En: *BBC NEWS*. Disponible en: https://www.bbc.com/news/world-latin-america-57359252

Torres Buelvas, J. E. (2019). Zonas grises y delincuencia organizada transnacional: Desafíos para la soberanía del estado en América Latina. En: *Revista Vía Iuris*. 27, pp. 318-349. https://doi.org/10.37511/viaiuris.n27a9

Vallés Causada, L. M. (2013). *La Policía Judicial en la obtención de inteligencia sobre comunicaciones electrónicas para el proceso penal*. Universidad Nacional de Educación a Distancia.

Vázquez Valdez, J. A. (2021). RTC, más que crimen organizado, cárteles o narcotráfico. En: *Secuencia*. 111. Dsiponible en: https://doi.org/10.18234/SECUENCIA.V0I111.1799

Voeten, T. (2020). *Mexican drug violence: hybrid warfare, predatory capitalism and the logic of cruelty.* (Xlibris Corporation, ed.). Disponible en: https://books.google.com/books/about/Mexican_Drug_Violence.html?hl=es&id=66MWEAAAQBAJ

Williams, H. J. y Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. Disponible en: https://doi.org/10.7249/RR1964

Yager, M. (2019). *Russian Strategic Intentions: A Strategic Multilayer Assessment (SMA) White Paper*. Disponible en: http://nsiteam.com/sma-publications/

Young, W. y Stebbins, D. (2016). A Rapidly Changing Urban Environment: How Commercial Technologies Can Affect Military Intelligence Operations. https://doi.org/10.7249/PE181

Zeigler, S. M. *et al*. (2021). Analysis of Russian Irregular Threats. Disponible en:. https://doi.org/10.7249/RR-A412-3

3. Páginas web

https://archive.org/

https://www.boe.es/

https://www.boe.es/boe/dias/2015/10/06/pdfs/BOE-A-2015-10725.pdf

https://books.google.es/

https://dialnet.unirioja.es/

https://doi.org/

https://ecfr.eu/

http://www.echr.coe.int/
http://eur-lex.europa.eu/
https://www.europol.europa.eu/
https://www.goodreads.com
http://www.marcialpons.es
https://pdfroom.com/
https://www.nato.int/
http://www.studynet.herts.ac.uk/
https://www.unodc.org/
https://www.wiley.com/